LOCH TECHNOLOGIES

Government Solutions

Zero Trust Security for Wireless Edge-located Assets

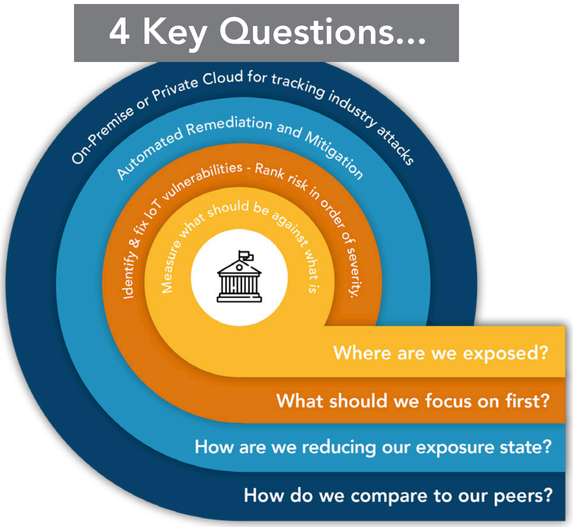
Zero Trust Security for Wireless Edge-located Assets

With 80% of new IoT deployments wireless, wireless is the new network and the new attack surface.

IoT has created the world's largest attack surface, the scope of which is only broadening with exponential growth in deployment of 5G/LTE. Today's networks and organizations were never built to handle this extraordinary volume, velocity, and hyperconnectivity of IoT technologies in the modern enterprise. This reality has created two critical security gaps for government organizations hoping to benefit from the promise of IoT products, applications, and services.

The LOCH Wireless Machine Vision™ platform provides next-generation wireless AI driven threat intelligence across 3G/4G and 5G deployments, broad-spectrum wireless IoT, Citizens Broadband Radio Service (CBRS) as well as 802.11/Bluetooth WiFi environments by providing customers with full IoT discovery, asset classification, risk analysis and actionable remediation capabilities based on a Zero Trust framework.

4 Key Questions...



On-Premise or Private Cloud for tracking industry attacks

Automated Remediation and Mitigation

Identify & fix IoT vulnerabilities - Rank risk in order of severity.

Measure what should be against what is

Where are we exposed?

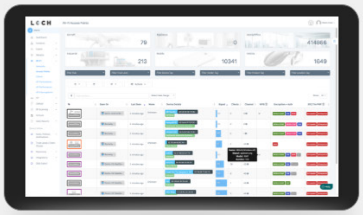
What should we focus on first?

How are we reducing our exposure state?

How do we compare to our peers?

Solution Benefits

DETECT

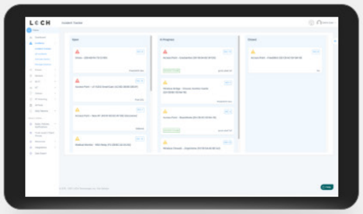


- Detect, identify & classify all broad spectrum RF emitting devices in range
- Device and network pairing communication map analysis and correlation
- Risk assessment threat ranking for Zero Trust network access control
- Mobile App for hunting rogues even if mobile

TRACK

- Wireless deep packet inspection
- Behavioral baselining, analysis and anomaly detection/alerts
- DVR-like capabilities for forensics, including geo-positioning
- Carrier integration with cellular devices for anomaly detection, fraud/ theft and cost management

REMEDIATE



- List & map devices on dashboard or directly into SIEMs.
- Interact with MDM & EMM assets for correlation & feedback on exceptions
- Rectify network segmentation via interactions with SOAR, FW and/or NAC systems
- Automate response & closure via collaboration with ITSM/ITSL & CMDBs

Rogue Cell Tower Detection - Prevent authorized devices from connecting to unauthorised cell towers

Detect and Prevent Evil Twin Attacks - Prevent authorized devices from connecting to unauthorised Wi-Fi Access Points

Roaming - prevent increase in data usage and excessive billing. Monitor potential data exfiltration against traffic base line to flag malware and bots.

Prevent Device Threats - Malware, Firmware Hacks, Sensor IoT Compromises, Man In the Middle Attacks, Device Tampering

Key Differentiators

- **Single pane of glass** to manage ALL wireless threats across cellular 3G/4G/5G, broad-spectrum wireless, CBRS and 802.11/ Bluetooth Wi-Fi devices
- **Early Warning System** - detecting threats before they hit the wired network
- **Edge IoT Vulnerability Scanning** to detect open ports & services to identify exposed threats before they are abused
- **Monitor Enforce Zero-**Trust Policies and "No Phone" Zones
- **Deployable** in air-gapped environments also
- **API driven integration** with wide ecosystem for automated remediation and collaboration

THIS REGISTRATION IS MAINTAINED BY USFCR VERIFIED VENDOR 2021

LOCH is proud to announce
that our solutions are now available to Federal Government Agencies via
'Simplified Acquisition Program (SAP)

Zero Trust Security for Multi Access Edge

5G/LTE, Broad Spectrum and Wireless Wi-Fi Intrusion Detection
"INVISIBLE THREATS, VISIBLE PROTECTION."

LOCH TECHNOLOGIES

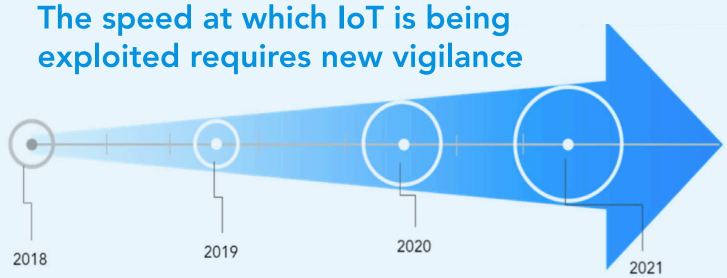
Invisible Threats. Visible Protection

Identify unmanaged, unsecured and misconfigured IoT devices within your environment

Use Cases for IoT in Government & Public Sector Are Everywhere

- Smart Cities & Buildings (GSA, DOT)
- Fleet Telematics (GSA, DoD, DHS)
- Asset Management (All)
- Enhance Military Capability (DARPA, DoD, DHS, DHA)
- Monitor Weather & Environment (NOAA)
- Protect Public Health & Safety (VA, USGS, DHS, CDC, FEMA, EPA)

The speed at which IoT is being exploited requires new vigilance



2018

- 83% of IoT run on unsupported operating systems

2019

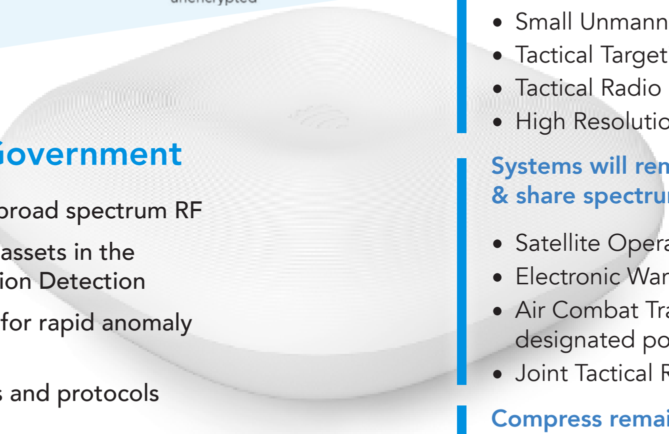
- 25 Billion IoT online
- 57% of IoT is vulnerable to high impact attacks that can lead to data exfiltration

2020

- 50 Billion IoT online
- IoT attacks every 1 min
- Cost of Breach $2.7M

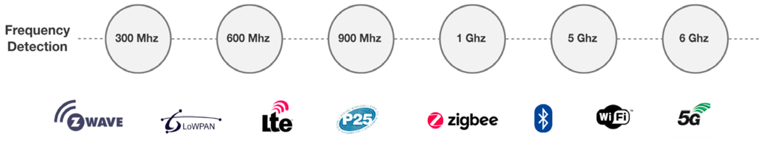
2021

- IoT attacks every 3 secs
- Cost of Breach $5.8M
- More attacks in 1H/21 than in all of 2020
- 98% of IoT traffic is unencrypted

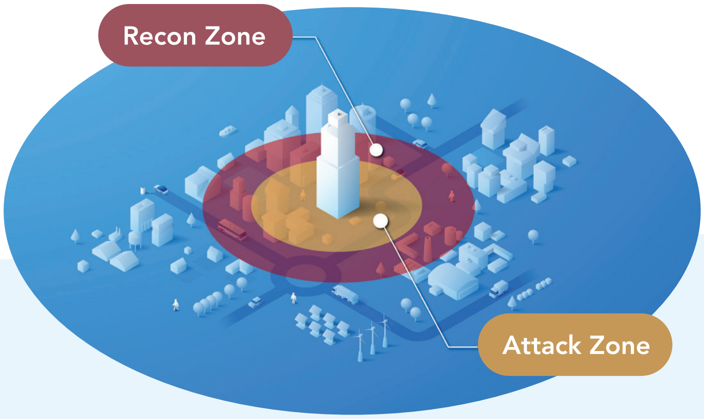


Core Competencies for Government

- Software defined radios to detect broad spectrum RF
- Comprehensive classification of all assets in the environment and continuous Intrusion Detection
- Wireless Security Threat Research for rapid anomaly detection
- Decoding of IoT operating systems and protocols (customizable for DoD)
- Zero-Trust Policy Enforcement
- Rogue Cellular Tower and Stingray Detection
- API integrations for threat mitigation & remediation



Wireless has created a new invisible attack surface



Business Drivers Leading Change

Sensors communicating over a wide range of RF is the "lynchpin" of IoT, especially pioneering DoD technology

Selected systems to operate at 1780-1850 and 2025-2110 MHz

- Small Unmanned Aerial Systems
- Tactical Targeting Network Technology
- Tactical Radio Relay
- High Resolution Video systems

Systems will remain in 1755-1780 MHz band & share spectrum

- Satellite Operations at 25 locations
- Electronic Warfare
- Air Combat Training System (within two designated polygons in the West)
- Joint Tactical Radio System at six key sites

Compress remaining 1755-1780 operations into 1780-1850 MHz

- Air Combat Training System
- Joint Tactical Radio System at all other sites
- Precision Guided Munitions
- Aeronautical Mobile Telemetry

Biden's Executive Order on Cybersecurity Highlights Zero Trust Security

https://www.whitehouse.gov/executive-order-on-improving-cybersecurity/

info@loch.io | 1-888-725-9434 | www.loch.io